

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-91883
(P2002-91883A)

(43) 公開日 平成14年3月29日 (2002.3.29)

(51) Int.Cl. ⁷	識別記号	F I	ターマート [*] (参考)
G 0 6 F 13/00	6 2 5	G 0 6 F 13/00	6 2 5 5 K 0 2 7
H 0 4 L 12/54		H 0 4 M 1/00	R 5 K 0 3 0
12/58		11/00	3 0 2 5 K 1 0 1
H 0 4 M 1/00		H 0 4 L 11/20	1 0 1 B
11/00	3 0 2		

審査請求 未請求 請求項の数11 O L (全 24 頁)

(21) 出願番号 特願2000-284861 (P2000-284861)

(22) 出願日 平成12年9月20日 (2000.9.20)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 太田 晴也

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

Fターム(参考) 5K027 AA11 BB09 HH00 MM03

5K030 GA19 HA06 HC09 JL01 JT01

JT02 JT09 KA01 KA02 LD13

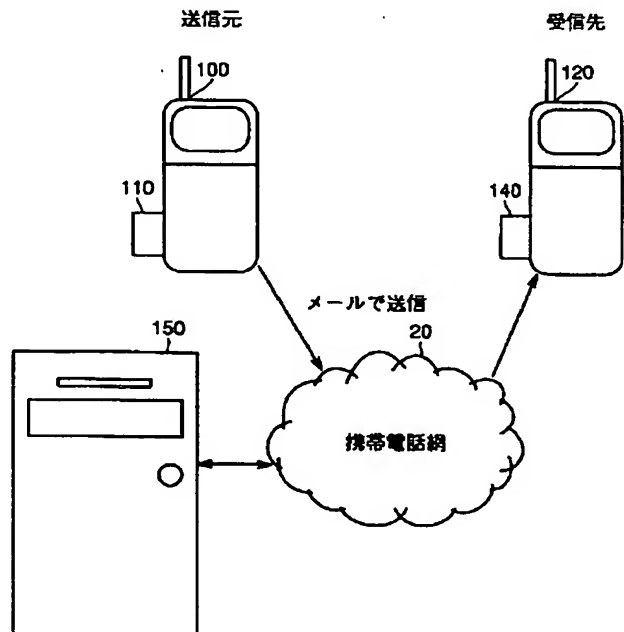
5K101 KK02 KK18 LL12 NN15

(54) 【発明の名称】 データ配信システムおよびデータ端末装置

(57) 【要約】

【課題】 ユーザ間でコンテンツ情報を自由にやり取りすることができるデータ配信システムおよびそのデータ配信システムに用いられるデータ端末装置を提供する。

【解決手段】 携帯電話機100は、コンテンツデータと、コンテンツデータの関連情報であるコンテンツ情報とを含むコンテンツファイルをサーバからダウンロードし、装着されたメモ리카ード110に記録する。そして、携帯電話機100は、メモ리카ード110からコンテンツ情報を読み出し、その読み出したコンテンツ情報をメール文に付加したコンテンツメールを作成し、携帯電話網20およびメールサーバ150を介して携帯電話機120へ送信する。



【特許請求の範囲】

【請求項 1】 コンテンツデータをファイル形式によって保持するコンテンツファイルと、前記コンテンツファイルを利用するためのライセンスとを保持するサーバと、

前記サーバから前記コンテンツファイルおよび前記ライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、前記コンテンツファイルに含まれるコンテンツ情報をメール文に付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、
前記コンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成るデータ配信システム。

【請求項 2】 コンテンツデータをファイル形式によって保持するコンテンツファイルと、前記コンテンツファイルを利用するためのライセンスとを保持するサーバと、

前記サーバから前記コンテンツファイルおよび前記ライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、前記コンテンツファイルに含まれるコンテンツ情報とコンテンツ ID とをタグとともにメールに付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、
前記コンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成るデータ配信システム。

【請求項 3】 コンテンツデータをファイル形式によって保持するコンテンツファイルと、前記コンテンツファイルを利用するためのライセンスとを保持するサーバと、

前記サーバから前記コンテンツファイルおよび前記ライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、前記コンテンツファイルに含まれるコンテンツ情報とコンテンツ ID とをタグとともにメールに付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、
前記コンテンツメールを受信し、その受信したコンテンツメールに含まれるコンテンツ ID を前記サーバへ送信して前記サーバから前記コンテンツ ID によって特定されるコンテンツファイルをダウンロードする他の端末装置と、

前記メールサーバから前記コンテンツメールを受信し、その受信したコンテンツメールを前記他の端末装置へ送信するメールサーバとから成るデータ配信システム。

【請求項 4】 前記データ端末装置は、前記他の端末装置からのコンテンツ情報の送信要求に応じて前記コンテンツメールを出力する、請求項 1 から請求項 3 のいずれか 1 項に記載のデータ配信システム。

【請求項 5】 前記データ端末装置は、ユーザによって入力されたコンテンツ情報の送信要求に応じて前記コンテンツメールを出力する、請求項 1 から請求項 3 のいずれか 1 項に記載のデータ配信システム。

【請求項 6】 コンテンツデータをファイル形式によって保持するコンテンツファイルと、前記コンテンツファイルを利用するためのライセンスとをサーバからダウンロードしてデータ記録装置に記録し、前記コンテンツファイルに含まれるコンテンツ情報を他の端末装置へ送信するデータ端末装置であって、

バスと、
前記バスに接続され、前記データ記録装置と前記バスとの間でデータのやり取りを制御するインタフェースと、
前記バスに接続され、外部と通信を行なう送受信部と、
前記バスに接続され、情報を入力するためのキー操作部と、

前記バスに接続され、前記他の端末装置へ送信するためのメールを作成するメール作成部と、
前記バスに接続された制御部とを備え、
前記コンテンツファイルのダウンロード時、
前記制御部は、前記キー操作部から入力された前記コンテンツファイルのダウンロード要求に応じて、前記コンテンツデータを特定するためのコンテンツ ID を前記サーバへ送信するように前記送受信部を制御し、前記送受信部が受信したコンテンツファイルおよびライセンスを前記インタフェースを介して前記データ記録装置へ出力し、

前記送受信部は、前記制御部からの制御により前記コンテンツ ID を前記サーバへ送信し、前記コンテンツファイルおよび前記ライセンスを受信し、
前記コンテンツ情報の送信時、
前記制御部は、コンテンツ情報の送信要求に応じて、前記インタフェースを介して前記データ記録装置からコンテンツ情報を取得し、その取得したコンテンツ情報を前記メール作成部へ与え、前記メール作成部から出力された前記コンテンツ情報を含むコンテンツメールを前記他の端末装置へ送信するように前記送受信部を制御し、
前記メール作成部は、前記コンテンツ情報をメール文に付加したコンテンツメールを作成し、
前記送受信部は、前記制御部からの制御によって前記コンテンツメールを前記他の装置へ送信する、データ端末装置。

【請求項 7】 前記コンテンツ情報の送信時、
前記制御部は、前記キー操作部から入力されたコンテンツ情報の送信要求に応じて、前記コンテンツ情報を前記データ記録装置から取得する、請求項 6 に記載のデータ

端末装置。

【請求項 8】 前記コンテンツ情報の送信時、前記制御部は、前記送受信部が受信したコンテンツ情報の送信要求に応じて、前記コンテンツ情報を前記データ記録装置から取得する、請求項 6 に記載のデータ端末装置。

【請求項 9】 前記コンテンツ情報の送信時、前記制御部は、前記インタフェースを介して複数のデータ記録装置からコンテンツ情報を取得し、前記メール作成部へ与える、請求項 6 から請求項 8 のいずれか 1 項に記載のデータ端末装置。

【請求項 10】 前記コンテンツ情報の送信時、前記制御部は、前記インタフェースを介してユーザが保持する全てのデータ記録装置からコンテンツ情報を取得し、前記メール作成部へ与える、請求項 6 から請求項 8 のいずれか 1 項に記載のデータ端末装置。

【請求項 11】 前記コンテンツ情報の送信時、前記制御部は、前記コンテンツ情報とともにコンテンツ ID を前記インタフェースを介して前記データ記録装置から取得し、前記コンテンツ情報およびコンテンツ ID を前記メール作成部へ与え、前記メール作成部は、前記コンテンツ情報およびコンテンツ ID をタグとともにメール文に付加してコンテンツメールを作成する、請求項 6 から請求項 10 のいずれか 1 項に記載のデータ端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システム、およびそのデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著

作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとりて考えて見ると、通常販売されている音楽データを記録した CD（コンパクトディスク）については、CD から光磁気ディスク（MD 等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体や MD 等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CD から MD へデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能な MD からさらに他の MD に音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書とを暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスキーを送信する。そして、暗号化コンテンツデータやライセンスキーを配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化されたライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンスキーと暗号化コンテンツデ

ータをメモリに記録する。

【0012】そして、メモリに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。そして、携帯電話機のユーザは、受信した暗号化コンテンツデータを再生した結果、その暗号化コンテンツデータを他人にプレゼントしたい場合がある。また、他人が持っている暗号化コンテンツデータを貰いたい場合もある。さらに、暗号化コンテンツデータに限らず、暗号化されていない平文のコンテンツデータについても、他人との間でやり取りを行ないたい場合がある。

【0014】

【発明が解決しようとする課題】しかし、コンテンツデータを配信する従来のシステムにおいては、サーバからダウンロードしたコンテンツデータのタイトル、およびアーティスト名等、コンテンツデータの関連情報であるコンテンツ情報を他人に送信したり、他人から受信したりすることがなく、ユーザ間でコンテンツ情報をやり取りすることができないという問題があった。

【0015】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、ユーザ間でコンテンツ情報を自由にやり取りすることができるデータ配信システムおよびそのデータ配信システムに用いられるデータ端末装置を提供することである。

【0016】

【課題を解決するための手段および発明の効果】この発明によるデータ配信システムは、コンテンツデータをファイル形式によって保持するコンテンツファイルと、コンテンツファイルを利用するためのライセンスとを保持するサーバと、サーバからコンテンツファイルおよびライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、コンテンツファイルに含まれるコンテンツ情報をメール文に付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、コンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成る。

【0017】この発明によるデータ配信システムにおいては、データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録および／または再生を行なう。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報を取得し、そのコンテンツ情報

をメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールをメールサーバを介して他の端末装置へ送信する。

【0018】したがって、この発明によれば、データ端末装置は、自動的にコンテンツメールを作成し、他の端末装置へコンテンツメールを送信するので、表示機能や操作機能の乏しい端末装置におけるユーザの負荷を軽減できる。

【0019】また、この発明によるデータ配信システムは、コンテンツデータをファイル形式によって保持するコンテンツファイルと、コンテンツファイルを利用するためのライセンスとを保持するサーバと、サーバからコンテンツファイルおよびライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、コンテンツファイルに含まれるコンテンツ情報とコンテンツIDとをタグとともにメールに付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、コンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成る。

【0020】この発明によるデータ配信システムにおいては、データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録および／または再生を行なう。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報と、コンテンツデータを特定するためのコンテンツIDとを取得し、そのコンテンツ情報およびコンテンツIDをタグとともにメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールをメールサーバを介して他の端末装置へ送信する。

【0021】したがって、この発明によれば、データ端末装置は、自動的にコンテンツメールを作成し、他の端末装置へコンテンツメールを送信するので、表示機能や操作機能の乏しい端末装置におけるユーザの負荷を軽減できるとともに、コンテンツメールを受取った他の端末装置のユーザはタグに基づいてコンテンツデータの配信をサーバへ要求することができる。その結果、ユーザの負荷を一層軽減できる。

【0022】また、この発明によるデータ配信システムは、コンテンツデータをファイル形式によって保持するコンテンツファイルと、コンテンツファイルを利用するためのライセンスとを保持するサーバと、サーバからコンテンツファイルおよびライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、コンテンツファイルに含まれるコンテンツ情報とコンテンツIDとをタグとともにメールに付加してコ

ンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、コンテンツメールを受信し、その受信したコンテンツメールに含まれるコンテンツIDをサーバへ送信してサーバからコンテンツIDによって特定されるコンテンツファイルをダウンロードする他の端末装置と、メールサーバからコンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成る。

【0023】この発明によるデータ配信システムにおいては、データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録および／または再生を行なう。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報と、コンテンツデータを特定するためのコンテンツIDとを取得し、そのコンテンツ情報およびコンテンツIDをタグとともにメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールをメールサーバを介して他の端末装置へ送信する。

【0024】そうすると、他の端末装置は、コンテンツメールを受信し、コンテンツメールに含まれるコンテンツIDをタグを手がかりにしてサーバへ送信してコンテンツIDによって特定されるコンテンツファイルをダウンロードする。

【0025】したがって、この発明によれば、コンテンツメールを受信した他の端末装置のユーザは、コンテンツIDを取得しなくても、コンテンツファイルをダウンロードできる。

【0026】好ましくは、データ端末装置は、他の端末装置からのコンテンツ情報の送信要求に応じてコンテンツメールを出力する。

【0027】データ端末装置は、他の端末装置からのコンテンツ情報の送信要求を受信すると、コンテンツ情報を含むコンテンツメールを作成し、他の端末装置へコンテンツメールを送信する。

【0028】したがって、この発明によれば、他のユーザからの要求に応じてコンテンツ情報を送信できる。その結果、他のユーザはサーバへアクセスしなくてもコンテンツ情報を容易に取得できる。

【0029】好ましくは、データ端末装置は、ユーザによって入力されたコンテンツ情報の送信要求に応じてコンテンツメールを出力する。

【0030】データ端末装置は、コンテンツ情報の送信要求が入力されると、コンテンツ情報を含むコンテンツメールを作成し、他の端末装置へコンテンツメールを送信する。

【0031】したがって、この発明によれば、ユーザは自己の有するコンテンツデータに関するコンテンツ情報を他のユーザに知らせることができる。

【0032】また、この発明によるデータ端末装置は、コンテンツデータをファイル形式によって保持するコンテンツファイルと、コンテンツファイルを利用するためのライセンスとをサーバからダウンロードしてデータ記録装置に記録し、コンテンツファイルに含まれるコンテンツ情報を他の端末装置へ送信するデータ端末装置であって、バスと、バスに接続され、データ記録装置とバスとの間でデータのやり取りを制御するインタフェースと、バスに接続され、外部と通信を行なう送受信部と、バスに接続され、情報を入力するためのキー操作部と、バスに接続され、他の端末装置へ送信するためのメールを作成するメール作成部と、バスに接続された制御部とを備え、コンテンツファイルのダウンロード時、制御部は、キー操作部から入力されたコンテンツファイルのダウンロード要求に応じて、コンテンツデータを特定するためのコンテンツIDをサーバへ送信するように送受信部を制御し、送受信部が受信したコンテンツファイルおよびライセンスをインタフェースを介してデータ記録装置へ出力し、送受信部は、制御部からの制御によりコンテンツIDをサーバへ送信し、コンテンツファイルおよびライセンスを受信し、コンテンツ情報の送信時、制御部は、コンテンツ情報の送信要求に応じて、インタフェースを介してデータ記録装置からコンテンツ情報を取得し、その取得したコンテンツ情報をメール作成部へ与え、メール作成部から出力されたコンテンツ情報を含むコンテンツメールを他の端末装置へ送信するように送受信部を制御し、メール作成部は、コンテンツ情報をメール文に付加したコンテンツメールを作成し、送受信部は、制御部からの制御によってコンテンツメールを他の装置へ送信する。

【0033】データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録する。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報を取得し、そのコンテンツ情報をメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールを他の端末装置へ送信する。

【0034】したがって、この発明によれば、データ端末装置は、自動的にコンテンツメールを作成し、他の端末装置へコンテンツメールを送信するので、表示機能や操作機能の乏しい端末装置におけるユーザの負荷を軽減できる。

【0035】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、キー操作部から入力されたコンテンツ情報の送信要求に応じて、コンテンツ情報をデータ記録装置から取得する。

【0036】データ端末装置においては、キー操作部からコンテンツ情報の送信要求に応じてコンテンツ情報を

データ記録装置から取得し、メール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールを他の端末装置へ送信する。

【0037】したがって、この発明によれば、データ端末装置のユーザは、自己の有するコンテンツデータに関するコンテンツ情報を他のユーザに知らせることができる。

【0038】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、送受信部が受信したコンテンツ情報の送信要求に応じて、コンテンツ情報をデータ記録装置から取得する。

【0039】データ端末装置は、他の端末装置からのコンテンツ情報の送信要求を受信すると、コンテンツ情報を含むコンテンツメールを作成し、他の端末装置へコンテンツメールを送信する。

【0040】したがって、この発明によれば、他のユーザからの要求に応じてコンテンツ情報を送信できる。その結果、他のユーザはサーバへアクセスしなくてもコンテンツ情報を容易に取得できる。

【0041】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、インタフェースを介して複数のデータ記録装置からコンテンツ情報を取得し、メール作成部へ与える。

【0042】データ端末装置は、複数のデータ記録装置に記録された全てのコンテンツデータに関するコンテンツ情報をメール文に付加してコンテンツメールを作成し、その作成したコンテンツメールを他の端末装置へ送信する。

【0043】したがって、この発明によれば、複数のデータ記録装置に記録されたコンテンツデータに関するコンテンツ情報を他の端末装置へ送信できる。

【0044】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、インタフェースを介してユーザが保持する全てのデータ記録装置からコンテンツ情報を取得し、メール作成部へ与える。

【0045】データ端末装置は、ユーザが保持する全てのコンテンツデータに関するコンテンツ情報をメール文に付加してコンテンツメールを作成し、その作成したコンテンツメールを他の端末装置へ送信する。

【0046】したがって、この発明によれば、ユーザが保持する全てのコンテンツデータに関するコンテンツ情報を他の端末装置へ送信できる。

【0047】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、コンテンツ情報とともにコンテンツIDをインタフェースを介してデータ記録装置から取得し、コンテンツ情報およびコンテンツIDをメール作成部へ与え、メール作成部は、コンテンツ情報およびコンテンツIDをタグとともにメール文に付加してコンテンツメールを作成する。

【0048】データ端末装置は、サーバからコンテンツ

データを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録および/または再生を行なう。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報と、コンテンツデータを特定するためのコンテンツIDとを取得し、そのコンテンツ情報およびコンテンツIDをタグとともにメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールをメールサーバを介して他の端末装置へ送信する。

【0049】したがって、この発明によれば、データ端末装置は、自動的にコンテンツメールを作成し、他の端末装置へコンテンツメールを送信するので、表示機能や操作機能の乏しい端末装置におけるユーザの負荷を軽減できるとともに、コンテンツメールを受取った他の端末装置のユーザはタグに基づいてコンテンツデータの配信をサーバへ要求することができる。その結果、ユーザの負荷を一層軽減できる。

【0050】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0051】図1は、本発明によるデータ配信システムにおける暗号化コンテンツデータのメモリカードへの配信を概念的に説明するための概略図である。

【0052】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば静止画、動画等の画像データ等を配信する場合においても適用することが可能なものである。

【0053】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【0054】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して、暗号化コンテンツデータとライ

センスとを配信する。

【0055】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0056】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0057】以下では、このようなライセンスサーバ10と配信キャリア20とを併せて、配信サーバ30と総称することにする。

【0058】また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0059】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0060】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0061】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0062】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生装置（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0063】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0064】まず、配信サーバ30より配信されるデー

タについて説明する。Dataは、音楽データ等のコンテンツデータである。コンテンツデータDataには、ライセンスキーKcで復号可能な暗号化が施される。ライセンスキーKcによって復号可能な暗号化が施された暗号化コンテンツデータ{Data}Kcがこの形式で配信サーバ30より携帯電話ユーザに配布される。

【0065】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

10 【0066】さらに、配信サーバ30からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Data-infが配布される。また、ライセンス情報としては、コンテンツデータDataを識別するためのコードであるコンテンツIDおよびライセンスの発行を特定できる管理コードであるライセンスIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1および再生回路における制御情報である再生回路制御情報AC2等が存在する。以後、ライセンスキーKcとコンテンツIDとライセンスIDとアクセス制御情報AC1と再生回路制御情報AC2とを併せて、ライセンスと総称することとする。

【0067】図3は、図1に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

30 【0068】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるよう禁止クラスリストCRL(Class Revocation List)の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0069】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機およびメモリカードのクラスをリストアップした禁止クラスリストデータCRLが含まれる。

40 【0070】禁止クラスリストデータCRLは、配信サーバ30内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データCRL-datを配信サーバ30側より発生して、これに応じてメモリカード内の禁止クラスリストCRLが置換えられる構成とする。また、禁止クラスリストのバージョンについては、CRL-verをメモリカード側より出力し、これを配信サーバ30側

で確認することによってバージョン管理を実行する。差分データ CRL_data には新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【0071】このように、禁止クラスリスト CRL を、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードへのライセンスキーの供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【0072】このように、メモリカード内の禁止クラスリスト CRL は配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリスト CRL の管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール (Tamper Resistance Module) に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータ CRL を改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【0073】コンテンツ再生回路 (携帯電話機) およびメモリカードには固有の公開暗号鍵 K_{Ppn} および K_{Pmc i} がそれぞれ設けられ、公開暗号鍵 K_{Ppn} および K_{Pmc i} はコンテンツ再生回路に固有の秘密復号鍵 K_{p n} およびメモリカード固有の秘密復号鍵 K_{m c i} によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生回路の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【0074】また、コンテンツ再生回路およびメモリカードのクラス証明書として、C_{r t f n} および C_{m c i} がそれぞれ設けられる。

【0075】これらのクラス証明書は、メモリカードおよびコンテンツ再生回路 (携帯電話機) のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【0076】これらのメモリカードおよびコンテンツ再生回路固有の公開暗号鍵およびクラス証明書は、認証データ {K_{Pmc i} / C_{m c i}} K_{Pma} および {K_{Ppn} / C_{r t f n}} K_{Pma} の形式で、出荷時にメモリカードおよび携帯電話機のコンテンツ再生回路にそれぞれ記録される。後ほど詳細に説明するが、K_{Pma} は配信システム全体で共通の公開認証鍵である。

【0077】図 4 は、図 1 に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図

である。

【0078】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ 30、携帯電話機 100、メモリカード 110 において生成される共通鍵 K_{s 1} ~ K_{s 3} が用いられる。

【0079】ここで、共通鍵 K_{s 1} ~ K_{s 3} は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 K_{s 1} ~ K_{s 3} を「セッションキー」とも呼ぶこととする。

【0080】これらのセッションキー K_{s 1} ~ K_{s 3} は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキー K_{s 1} は、配信サーバによって配信セッションごとに発生される。セッションキー K_{s 2} は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキー K_{s 3} は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0081】また、メモリカード 110 内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵 K_{Pm} と、公開暗号鍵 K_{Pm} で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 K_m が存在する。

【0082】図 5 は、図 1 に示したライセンスサーバ 10 の構成を示す概略ブロック図である。

【0083】ライセンスサーバ 10 は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンス ID 等の配信情報を保持するための情報データベース 304 と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース 302 と、禁止クラスリスト CRL を管理する CRL データベース 306 と、情報データベース 304、課金データベース 302 および CRL データベース 306 からのデータをバス BS1 を介して受取り、所定の処理を行なうためのデータ処理部 310 と、通信網を介して、配信キャリア 20 とデータ処理部 310 との間でデータ授受を行なうための通信装置 350 とを備える。

【0084】データ処理部 310 は、バス BS1 上のデータに応じて、データ処理部 310 の動作を制御するための配信制御部 315 と、配信制御部 315 に制御されて、配信セッション時にセッションキー K_{s 1} を発生す

るためのセッションキー発生部 316 と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ {K P m c i / C m c i} K P m a を通信装置 350 およびバス B S 1 を介して受けて、公開認証鍵 K P m a による復号処理を行なう復号処理部 312 と、セッションキー発生部 316 より生成されたセッションキー K s 1 を復号処理部 312 によって得られた公開暗号鍵 K P m c m を用いて暗号化して、バス B S 1 に出力するための暗号化処理部 318 と、セッションキー K s 1 によって暗号化された上で送信されたデータをバス B S 1 より受けて、復号処理を行なう復号処理部 320 とを含む。

【0085】データ処理部 310 は、さらに、配信制御部 315 から与えられるライセンスキー K c および再生回路制御情報 A C 2 を、復号処理部 320 によって得られたメモリカード固有の公開暗号鍵 K P m によって暗号化するための暗号化処理部 326 と、暗号化処理部 326 の出力を、復号処理部 320 から与えられるセッションキー K s 2 によってさらに暗号化してバス B S 1 に出力するための暗号化処理部 328 とを含む。

【0086】ライセンスサーバ 10 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0087】図 6 は、図 5 に示す情報データベース 304 に保持されるコンテンツファイルを示したものである。情報データベース 304 は、複数の記録媒体 40 を有する。記録媒体 40 は、コンテンツファイル (Content File) 1 ~ コンテンツファイル 5 等の複数のコンテンツファイル 41 を含む。

【0088】図 7 は、記録媒体 40 に含まれるコンテンツファイル 41 の構成を示したものである。コンテンツファイル 41 は、ファイルヘッダ (File Header) 410、コンテンツ情報 (Content Information) 420、コンテンツテーブル (Table of Data Objects) 430、およびコンテンツデータ (Data Objects) 1 (440) ~ コンテンツデータ N (44n) から成る。コンテンツデータ 440 ~ 44n の各々は、ライセンスキー K c によって復号可能なように暗号化されている。

【0089】ファイルヘッダ 410 は、コンテンツを配信する配信プロトコルの固有識別情報である U D A C Code 411 と、プロトコルのバージョン番号を示す Protocol Version 412 と、コンテンツの固有識別子である Content ID 413 と、コンテンツのバージョン番号を示す Content Version 414 と、ファイルのバイトサイズを示す File Length 415 と、コンテンツの種類を示す Content Type 416 と、コンテンツの再生時間を示す Play Time 417 と、コンテンツ

データの数を示す Number of Data Objects 418 と、コンテンツ情報 420 のバイトサイズを示す Information Length 419 とから構成される。

【0090】また、コンテンツ情報 420 は、曲名 421 およびアーティスト名 422 とから構成され、コンテンツデータ 440 ~ 44n に関連する情報が含まれる。コンテンツテーブル 430 は、コンテンツデータ 440 ~ 44n の各々のファイル上の位置やサイズ情報である。コンテンツデータ 440 ~ 44n は、コンテンツの実体である音楽や歌詞データである。図 7 に示すファイル構成によって 1 つのコンテンツファイルが構成される。また、コンテンツデータ 440 ~ 44n によって 1 つのコンテンツデータが構成される。つまり、コンテンツデータ 440 ~ 44n によって 1 つのコンテンツデータ {Data} K c を構成する。したがって、携帯電話機 100 のユーザからコンテンツデータ {Data} K c の配信要求があったときは、そのコンテンツデータ {Data} K c が含まれるコンテンツファイルが携帯電話機 100 に配信される。

【0091】図 8 は、図 1 に示した携帯電話機 100 の構成を説明するための概略ブロック図である。

【0092】携帯電話機 100 は、携帯電話網により無線伝送される信号を受信するためのアンテナ 1102 と、アンテナ 1102 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、携帯電話機 100 の各部のデータ授受を行なうためのバス B S 2 と、バス B S 2 を介して携帯電話機 100 の動作を制御するためのコントローラ 1106 とを含む。

【0093】携帯電話機 100 は、さらに、外部からの指示を携帯電話機 100 に与えるためのキー操作部 1108 と、コントローラ 1106 等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データベース B S 2 を介して与えられる受信データに基づいて音声再生するための音声再生部 1112 とを含む。ここで、携帯電話機 (コンテンツ再生回路) 100 のクラス n は、n = 1 であるとする。

【0094】携帯電話機 100 は、さらに、音声再生部 1112 の出力をディジタル信号からアナログ信号に変換する D A 変換器 1113 と、D A 変換器 1113 の出力を外部出力装置等へ出力するための端子 1114 とを含む。

【0095】携帯電話機 100 は、さらに、配信サーバ 30 からのコンテンツデータ (音楽データ) を記憶しかつ復号化処理するための着脱可能なメモリカード 110 と、メモリカード 110 とバス B S 2 との間のデータの授受を制御するためのメモリインタフェース 1200 と

を含む。

【0096】携帯電話機100は、さらに、携帯電話機の種類(クラス)ごとにそれぞれ設定される、公開暗号鍵K P p 1およびクラス証明書C r t f 1を公開復号鍵K P m aで復号することでその正当性を認証できる状態に暗号化した認証データ{K P p 1/C r t f 1} K P m aを保持する認証データ保持部1202を含む。

【0097】携帯電話機100は、さらに、携帯電話機(コンテンツ再生回路)固有の復号鍵であるK p 1を保持するK p 1保持部1204と、バスB S 2から受けたデータをK p 1によって復号しメモリカード110によって発生されたセッションキーK s 2を得る復号処理部1206とを含む。

【0098】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスB S 2上においてやり取りされるデータを暗号化するためのセッションキーK s 3を乱数等により発生するセッションキー発生部1210と、生成されたセッションキーK s 3を復号処理部1206によって得られたセッションキーK s 2によって暗号化しバスB S 2に出力する暗号化処理部1208とを含む。

【0099】携帯電話機100は、さらに、バスB S 2上のデータをセッションキーK s 3によって復号して出力する復号処理部1212とを含む。

【0100】携帯電話機100は、さらに、バスB S 2より暗号化コンテンツデータ{D a t a} K cを受けて、復号処理部1212より取得したライセンスキーK cによって復号しコンテンツデータを出力する復号処理部1214と、復号処理部1214の出力を受けてコンテンツデータを再生するための音楽再生部1216と、音楽再生部1216の出力をデジタル信号からアナログ信号に変換するD A変換器1218と、D A変換器1113とD A変換器1218との出力を受けて、動作モードに応じて選択的に端子1114または端子1220から出力するためのスイッチ1222と、スイッチ1222の出力を受けて、ヘッドホン130と接続するための接続端子1224とを含む。

【0101】携帯電話機100は、さらに、配信サーバ10から配信されたコンテンツデータのコンテンツ情報420をメール文に付加してコンテンツメールを作成するメール作成部1226を含む。

【0102】なお、図8においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生と、コンテンツメールの作成とにかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【0103】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0104】図9は、メモリカード110の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、K P m c iおよびK m c iが設けられ、メモリカードのクラス証明書C m c iが設けられるが、メモリカード110においては、これらは自然数 $i = 1$ でそれぞれ表わされるものとする。

【0105】したがって、メモリカード110は、認証データ{K P m c 1/C m c 1} K P m aを保持する認証データ保持部1400と、メモリカードの種類ごとに設定される固有の復号鍵であるK m c 1を保持するK m c 保持部1402と、メモリカードごとに固有に設定される秘密復号鍵K m 1を保持するK m 1保持部1421と、K m 1によって復号可能な公開暗号鍵K P m 1を保持するK P m 1保持部1416とを含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵K P m c 1およびクラス証明書C m c 1を公開認証鍵K P m aで復号することでその正当性を認証できる状態に暗号化した認証データ{K P m c 1/C m c 1} K P m aとして保持する。

【0106】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

【0107】メモリカード110は、さらに、メモリーインタフェース1200との間で信号を端子1201を介して授受するバスB S 3と、バスB S 3にメモリーインタフェース1200から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵K m c 1をK m c 1保持部1402から受けて、配信サーバ30が配信セッションにおいて生成したセッションキーK s 1を接点P aに出力する復号処理部1404と、K P m a保持部1414から認証鍵K P m aを受けて、バスB S 3に与えられるデータからK P m aによる復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444によって選択的に与えられるデータを暗号化してバスB S 3に出力する暗号化処理部1406とを含む。

【0108】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーK s 2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーK s 2を復号処理部1408によって得られる公開暗号鍵K P p nもしくはK P m c iによって暗号化してバスB S 3に送出する暗号化処理部1410と、バスB S 3よりセッションキーK s 2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキ

一Ks2によって復号し、復号結果をバスBS4に送出する復号処理部1412とを含む。

【0109】メモリカード110は、さらに、バスBS3上のデータを公開暗号鍵Kpm1と対をなすメモリカード110固有の秘密復号鍵Km1によって復号するための復号処理部1422と、公開暗号鍵Kpm1で暗号化されている、ライセンスキーKc、再生回路制御情報AC2および再生情報（コンテンツID、ライセンスID、アクセス制御情報AC1）と、暗号化されていない禁止クラスリストのバージョン更新のための差分データCRL_datによって逐次更新される禁止クラスリストデータCRLとをバスBS4より受けて格納するとともに、暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infをバスBS3より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。

【0110】メモリカード110は、さらに、復号処理部1422によって得られるライセンスID、コンテンツIDおよびアクセス制限情報AC1を保持するためのライセンス情報保持部1440と、バスBS3を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420とを含む。

【0111】ライセンス情報保持部1440は、バスBS4との間でライセンスID、コンテンツIDおよびアクセス制限情報AC1のデータの授受が可能である。ライセンス情報保持部1440は、N個（N：自然数）のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

【0112】なお、図9において、実線で囲んだ領域は、メモリカード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）である。

【0113】もちろん、メモリ1415も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図9に示したような構成とすることで、メモリ1415中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ1415中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1415を設ける必要がないので、製造コストが低減されるという利点がある。

【0114】次に、図1に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【0115】図10および図11は、図1に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第1および第2のフローチャートである。

【0116】図10および図11においては、携帯電話ユーザが、メモリカード110を用いることで、携帯電話機100を介して配信サーバ30から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

10 【0117】まず、携帯電話ユーザの携帯電話機100から、携帯電話ユーザによるキー操作部1108のキーボタンの操作等によって、配信リクエストがなされる（ステップS100）。

【0118】メモリカード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ{Kpmc1//Cmc1}Kpmaが出力される（ステップS102）。

20 【0119】携帯電話機100は、メモリカード110からの認証のための認証データ{Kpmc1//Cmc1}Kpmaに加えて、コンテンツID、ライセンス購入条件のデータACとを配信サーバ30に対して送信する（ステップS104）。

【0120】配信サーバ30では、携帯電話機100からコンテンツID、認証データ{Kpmc1//Cmc1}Kpma、ライセンス購入条件のデータACを受信し（ステップS106）、復号処理部312においてメモリカード110から出力された認証データを公開認証鍵Kpmaで復号処理を実行する（ステップS108）。

30 【0121】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからの公開暗号鍵Kpmc1と証明書Cmc1を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップS110）。正当な認証データであると判断された場合、配信制御部315は、公開暗号鍵Kpmc1および証明書Cmc1を承認し、受理する。そして、次の処理（ステップS112）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵Kpmc1および証明書Cmc1を受理しないで処理を終了する（ステップS170）。

40 【0122】認証の結果、正規の機器であることが認識されると、配信制御部315は、次に、メモリカード110のクラス証明書Cmc1が禁止クラスリストCRLにリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップS170）。

【0123】一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップS112）。

【0124】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ30において、セッションキー発生部316は、配信のためのセッションキーKs1を生成する。セッションキーKs1は、復号処理部312によって得られたメモリカード110に対応する公開暗号鍵K

【0125】暗号化されたセッションキーKs1は、{Ks1}Kmc1として、バスBS1および通信装置350を介して外部に出力される（ステップS116）。

【0126】携帯電話機100が、暗号化されたセッションキー{Ks1}Kmc1を受信すると（ステップS118）、メモリカード110においては、メモリインタフェース1200を介して、バスBS3に与えられた

【0127】コントローラ1420は、配信サーバ30で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対して、メモリカード110において配信動作時に生成されるセッションキーKs2の生成を指示する。

【0128】また、配信セッションにおいては、コントローラ1420は、メモリカード110内のメモリ1415に記録されている禁止クラスリストの状態（バージョン）に関連する情報として、リストのバージョンデータCRL_verをメモリ1415から抽出してバスBS4に出力する。

【0129】暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1404より与えられるセッションキーKs1によって、切換スイッチ1444および1446の接点を順次切換えることによって与えられるセッションキーKs2、公開暗号鍵K

【0130】バスBS3に出力された暗号化データ{Ks2//Kpm1//CRL_ver}Ks1は、バスBS3から端子1201およびメモリインタフェース1200を介して携帯電話機100に出力され、携帯電話機100から配信サーバ30に送信される（ステップS124）。

【0131】配信サーバ30は、暗号化データ{Ks2//Kpm1//CRL_ver}Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、メモリカード110固有の公開暗号鍵Kpm1およびメモリカード110における禁止クラスリストのバージョンデータCRL_verを受信する（ステップS126）。

【0132】禁止クラスリストのバージョン情報CRL_verは、バスBS1を介して配信制御部315に送られ、配信制御部315は、受理したバージョンデータCRL_verに従って、当該CRL_verのバージョンとCRLデータベース306内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データCRL_datを生成する（ステップS128）。

【0133】さらに、配線制御部315は、ステップS106で取得したコンテンツIDおよびライセンス購入条件データACに従って、ライセンスID、アクセス制限情報AC1および再生回路制御情報AC2を生成する（ステップS130）。さらに、暗号化コンテンツデータを復号するためのライセンスキーKcを情報データベース304より取得する（ステップS132）。

【0134】図11を参照して、配信制御部315は、生成したライセンス、すなわち、ライセンスキーKc、再生回路制御情報AC2、ライセンスID、コンテンツID、およびアクセス制限情報AC1を暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110固有の公開暗号鍵Kpm1によってライセンスを暗号化する（ステップS136）。暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がバスBS1を介して供給する禁止クラスリストの差分データCRL_datとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データは、バスBS1および通信装置350を介して携帯電話機100に送信される（ステップS138）。

【0135】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0136】携帯電話機100は、送信された暗号化データ{ {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1//CRL_dat } Ks2を受信し（ステップS140）、メモリインタフェース1200を介してメモリカード110へ出力する。メモリカード110においては、メモリインタフェース1

200を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS3の受信データを復号しバスBS4に出力する(ステップS142)。

【0137】この段階で、バスBS4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1と、CRL_dataとが出力される。コントローラ1420の指示によって、暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、メモリ1415に記録される(ステップS144)。一方、暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンスのうち、メモリカード110内で参照されるライセンスID、コンテンツIDおよびアクセス制限情報AC1のみが受理される(ステップS146)。

【0138】コントローラ1420は、受理したCRL_dataに基づいて、メモリ1415内の禁止クラスリストデータCRLおよびそのバージョンを更新する(ステップS148)。さらに、ライセンスID、コンテンツIDおよびアクセス制限情報AC1については、ライセンス情報保持部1440に記録される(ステップS150)。

【0139】ステップS150までの処理がメモリ回路で正常に終了した段階で、携帯電話機100から配信サーバ30にコンテンツデータの配信要求がなされる(ステップS152)。

【0140】配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ{Data} Kcおよび付加情報Data-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する(ステップS154)。この場合、配信サーバ30は、情報データベース304の記録媒体40からファイルヘッダ410、コンテンツ情報420、およびデータテーブル430を付加情報Data-infとして取得する。つまり、配信サーバ30は、暗号化コンテンツデータ{Data} Kcが含まれる1つのコンテンツファイル[Data-inf(ファイルヘッダ410+コンテンツ情報420+データテーブル430)//{Data} Kc(コンテンツデータ440~44n)]を取得する。

【0141】携帯電話機100は、Data-inf/{Data} Kcを受信して、暗号化コンテンツデータ{Data} Kcおよび付加情報Data-infを受信する(ステップS156)。暗号化コンテンツデータ{Data} Kcおよび付加情報Data-infは、メモリインタフェース1200および端子1201

を介してメモリカード110のバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ{Data} Kcおよび付加情報Data-infがそのままメモリ1415に記録される(ステップS158)。つまり、図7に示すファイル構成によって暗号化コンテンツデータ{Data} Kcおよび付加情報Data-infがメモリ1415に記録される。

【0142】さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され(ステップS160)、配信サーバ30で配信受理を受信すると(ステップS162)、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され(ステップS164)、全体の処理が終了する(ステップS170)。

【0143】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信できた公開暗号鍵Kp1およびKmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kp1およびKmc1による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0144】次に、図12および図13を参照してメモリカード110に配信されたコンテンツデータの携帯電話機100における再生動作について説明する。図12を参照して、再生動作の開始とともに、携帯電話機100のユーザからキー操作部1108を介して再生指示が携帯電話機100にインプットされる(ステップS200)。そうすると、コントローラ1106は、バスBS2を介して認証データ保持部1202から認証データ{Kp1//Crtf1} KPmaを読み出し、メモリインタフェース1200を介してメモリカード110へ認証データ{Kp1//Crtf1} KPmaを入力する(ステップS201)。

【0145】そうすると、メモリカード110は、認証データ{Kp1//Crtf1} KPmaを受信する(ステップS202)。そして、メモリカード110の復号処理部1408は、受理した認証データ{Kp1//Crtf1} KPmaを、KPma保持部1414に保持された公開認証鍵KPmaによって復号し(ステップS203)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{Kp1//Crtf1} KPmaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS204)。復号できなかった場合、コントローラ1420は認証データ不受理の出力を

データBS3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する(ステップS206)。認証データが復号できた場合、コントローラ1420は、取得した証明書Crtf1がメモリ1415から読出した禁止クラスリストデータに含まれるか否かを判断する(ステップS205)。この場合、証明書Crtf1にはIDが付与されており、コントローラ1420は、受理した証明書Crtf1のIDが禁止クラスリストデータの中に存在するか否かを判別する。証明書Crtf1が禁止クラスリストデータに含まれると判断されると、コントローラ1420は認証データ不受理の出力をデータBS3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する(ステップS206)。

【0146】ステップS204において認証データが公開認証鍵Kpmaで復号できなかったとき、およびステップS205において受理した証明書Crtf1が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して認証データ不受理の出力を受けると、認証データ不受理のデータをディスプレイ1110に表示する(ステップS207)。

【0147】ステップS205において、証明書Crtf1が禁止クラスリストデータに含まれていないと判断されると、図13を参照して、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS208)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kpp1によって暗号化した{Ks2}Kp1をバスBS3へ出力する(ステップS209)。そうすると、コントローラ1420は、端子1201を介してメモリインタフェース1200へ{Ks2}Kp1を出力し、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して{Ks2}Kp1を取得する。そして、Kp1保持部1204は、秘密復号鍵Kp1を復号処理部1206へ出力する。

【0148】復号処理部1206は、Kp1保持部1204から出力された、公開暗号鍵Kpp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号処理部1208へ出力する(ステップS210)。そうすると、セッションキー発生部1210は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1208へ出力する(ステップS211)。暗号処理部1208は、セッションキー発生部1210からのセッションキーKs3を復号処理部1206からのセッションキーKs2によって暗号化して{Ks3}Ks2を

出力し、コントローラ1106は、バスBS2およびメモリインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する(ステップS212)。

【0149】メモリカード110の復号処理部1412は、端子1201およびバスBS3を介して{Ks3}Ks2を入力し、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、携帯電話機100で発生されたセッションキーKs3を取得する(ステップS213)。

【0150】セッションキーKs3の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報AC1を確認する(ステップS214)。

【0151】ステップS214においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数に制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS215)。一方、アクセス制限情報AC1によって再生回数が制限されていない場合においては、ステップS215はスキップされ、アクセス制御情報AC1は更新されることなく処理が次のステップ(ステップS216)に進行される。

【0152】また、ライセンス情報保持部1440内にリクエスト曲の当該コンテンツIDが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【0153】ステップS214において、当該再生動作において再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキーKcを含むライセンスの復号処理が実行される。具体的には、コントローラ1420の指示に応じて、メモリ1415からバスBS4に読出された暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1を復号処理部1422がメモリカード110固有の秘密復号鍵Km1によって復号し、再生処理に必要なライセンスキーKcと再生回路制御情報AC2がバスBS4上に得られる(ステップS216)。

【0154】得られたライセンスキーKcと再生回路制御情報AC2は、切換スイッチ1444の接点Pdを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点Pdを介して復号処理部1412より受けたセッションキーKs3によってバスBS4から受けたライセンスキーKcと再生回路制御情報AC2とを暗号化し、{Kc//AC2}Ks3をバスBS3に出力する(ステップS217)。

【0155】バスBS3に出力された暗号化データは、メモリインタフェース1200を介して携帯電話機100

0に送出される。

【0156】携帯電話機100においては、メモリインタフェース1200を介してバスBS2に伝達される暗号化データ{Kc//AC2}Ks3を復号処理部1212によって復号処理を行ない、ライセンスキーKcおよび再生回路制御情報AC2を受理する(ステップS218)。復号処理部1212は、ライセンスキーKcを復号処理部1214に伝達し、再生回路制御情報AC2をバスBS2に出力する。

【0157】コントローラ1106は、バスBS2を介して、再生回路制御情報AC2を受理して再生の可否の確認を行なう(ステップS219)。

【0158】ステップS219においては、再生回路制御情報AC2によって再生不可と判断される場合には、再生動作は終了される。

【0159】ステップS219において再生可能と判断された場合、コントローラ1106は、メモリインタフェース1200を介してメモリカード110に暗号化コンテンツデータ{Data}Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Data}Kcを取得し、バスBS3および端子1201を介してメモリインタフェース1200へ出力する(ステップS220)。

【0160】携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して暗号化コンテンツデータ{Data}Kcを取得し、バスBS2を介して暗号化コンテンツデータ{Data}Kcを復号処理部1214へ与える。そして、復号処理部1214は、暗号化コンテンツデータ{Data}Kcを復号処理部1212から出力されたコンテンツ鍵Kcによって復号してコンテンツデータDataを取得する(ステップS221)。

【0161】そして、復号されたコンテンツデータDataは音楽再生部1216へ出力され、音楽再生部1216は、コンテンツデータを再生し、DA変換器1218はデジタル信号をアナログ信号に変換して端子1220へ出力する。そして、スイッチ1222は端子1220を選択して音楽データは端子1224を介してヘッドホン130へ出力されて再生される(ステップS222)。これによって再生動作が終了する。

【0162】上述したように、携帯電話機100のユーザは、携帯電話機100を用いて配信サーバ30から暗号化コンテンツデータ{Data}Kcをメモリカード110に受信し、ライセンスキーKcによって暗号化コンテンツデータ{Data}Kcを復号して再生することができる。

【0163】本発明においては、携帯電話機100は、配信サーバ30から暗号化コンテンツデータ{Data}Kcをメモリカード110に受信した後、携帯電話

機100のユーザからの要求に応じて暗号化コンテンツデータ{Data}Kcのコンテンツ情報をメールに付加してコンテンツメールを作成し、その作成したコンテンツメールを他の携帯電話機に送信する。すなわち、図14を参照して、携帯電話機100は、携帯電話網20、およびメールサーバ150を介して携帯電話機120とメールのやり取りを行なう。

【0164】携帯電話機120は、図8に示す携帯電話機100の構成と同じ構成から成る。また、携帯電話機120には、メモリカード140が脱着可能であり、メモリカード140は図9に示すメモリカード110の構成と同じ構成から成る。携帯電話機100は、暗号化コンテンツデータ{Data}Kcのアーティスト名および曲名をメモリカード110から取得し、アーティスト名および曲名をメールに付加することによってコンテンツメールを作成する。そして、携帯電話機100は、作成したコンテンツメールを携帯電話機120へ送信するために携帯電話網20へ出力する。携帯電話機網20は、コンテンツメールをメールサーバ150へ送信し、メールサーバ150はコンテンツメールのヘッダ部に付けられたアドレスから携帯電話機120を特定する。そして、メールサーバ150は、特定した携帯電話機120へコンテンツメールを送信する。携帯電話機120は、コンテンツメールを受取り、その受取ったアーティスト名および曲名をディスプレイ1110に表示する。これにより、携帯電話機120のユーザは、携帯電話機100に装着されたメモリカード110に聴きたい音楽データが記録されているかどうかを知ることができる。

【0165】そして、携帯電話機120のユーザは、受信したコンテンツメールをディスプレイ1110に表示し、取得した暗号化コンテンツデータがあれば、配信サーバ30へ暗号化コンテンツデータの配信を要求する。そして、携帯電話機120は、受信した暗号化コンテンツデータと、その暗号化コンテンツデータを復号するためのライセンスキーとを装着されたメモリカード140へ記録および/または再生を行なう。

【0166】図15を参照して、携帯電話機100が携帯電話網20を介して携帯電話機120へコンテンツ情報をメールに付加したコンテンツメールを送信する動作について説明する。携帯電話機100のユーザからキー操作部1108を介してコンテンツ情報の配信要求が入力されると(S300)、コントローラ1106は、メモリインタフェース1200を介してメモリカード110のメモリ1415に記録されたファイルヘッダ410の読出しを要求する。メモリカード110のコントローラ1420は、端子1201、およびバスBS3を介してファイルヘッダ410の読出要求を受取り、メモリ1415からファイルヘッダ410を読出す。この場合、コントローラ1420は、メモリカード110上に構築されたファイルシステムの管理情報を参照してファイル

ヘッダ 410 を読出す。そして、コントローラ 1420 は、バス BS3 および端子 1201 を介して読出したファイルヘッダ 410 をメモリインタフェース 1200 へ出力する。そして、コントローラ 1106 は、ファイルヘッダ 410 を受取る（ステップ S302）。なお、アーティスト名および曲名は、コンテンツファイルのコンテンツ情報 420 に含まれるから、最初からコンテンツ情報 420 を読出すのが普通であるが、図 7 に示すファイル構成においては、ファイルヘッダ 410 を読出さなければ、コンテンツ情報 420 を読出すことができない構成になっている。

【0167】携帯電話機 100 のコントローラ 1106 は、ファイルヘッダ 410 を読出した後、コンテンツ情報 420 の読出要求をメモリインタフェース 1200 を介してメモリカード 110 へ出力する。そうすると、メモリカード 110 のコントローラ 1420 は、端子 1201 およびバス BS3 を介してコンテンツ情報 420 の読出要求を受取り、メモリカード 110 上に構築されたファイルシステムの管理情報を参照しながらメモリ 1415 からコンテンツ情報 420 を読出す。そして、コントローラ 1420 は、バス BS3 および端子 1201 を介してメモリインタフェース 1200 にコンテンツ情報 420 を出力する。携帯電話機 100 のコントローラ 1106 は、メモリインタフェース 1200 を介してコンテンツ情報 420 を受取り、バス BS2 を介してコンテンツ情報 420 をメール作成部 1226 へ出力する。

【0168】メール作成部 1226 は、コンテンツ情報 420 をバス BS2 を介して受取り、コンテンツ情報 420 であるアーティスト名および曲名を、字間、字体等を整えながらメール本体に付加してコンテンツメールを作成し、コンテンツメールを出力する（ステップ S304）。コントローラ 1106 は、メモリカード 110 に記録された全てのファイルヘッダを読出したか否かを判断する（ステップ S306）。メモリカード 110 に記録された全てのファイルヘッダ 410 が読出されていないとき、ステップ S302、S304、S306 が繰返される。そして、コンテンツメールに次々とコンテンツ情報 420 が追加される。

【0169】メモリカード 110 から全てのファイルヘッダ 410 が読出されたと判断されると、次に、コントローラ 1106 は、他のメモリカードについても処理するか否かを判断する（ステップ S308）。他のメモリカードも処理する場合、ステップ S302、S304、S306、S308 が繰返される。つまり、ステップ S302、S304、S306、S308 は、携帯電話機 100 のユーザが所有するメモリカードに含まれる全てのコンテンツ情報 420 を他の携帯電話機 120 へ送信するためのステップである。そして、コントローラ 1106 は、他のメモリカードは処理しないと判断すると、メール作成部 1226 から出力されたコンテンツメール

をバス BS2 を介して受取り、送受信部 1104 へコンテンツメールを出力する。そして、送受信部 1104 は、アンテナ 1102 を介してコンテンツメールを送信し、携帯電話網 20 はコンテンツメールをメールサーバ 150 へ送る。メールサーバ 150 は、コンテンツメールのアドレスに基づいて携帯電話機 120 を特定し、携帯電話網 20 を介してコンテンツメールを携帯電話機 120 へ送信する（ステップ S310）。これによってメールの送信動作が終了する（ステップ S312）。

【0170】コンテンツメールを受取った携帯電話機 120 のユーザは、携帯電話機 120 のディスプレイ 1110 に表示されたアーティストおよび曲名を見てダウンロードしたい暗号化コンテンツデータがあれば、配信サーバ 30 に対して希望する暗号化コンテンツデータの配信要求を行なう。携帯電話機 120 が配信サーバ 30 から暗号化コンテンツデータをダウンロードする動作は、図 10 および図 11 に示すフローチャートに従って行なわれる。

【0171】メモリカード 110 に記録された暗号化コンテンツデータのコンテンツ情報 420 を自動的に作成し、その作成したコンテンツメールを携帯電話機 100 から携帯電話機 120 へ送信することによって、表示機能や操作機能が貧弱な携帯電話機におけるユーザの負荷を軽減することができる。

【0172】本発明による暗号化コンテンツデータのコンテンツ情報 420 を他の携帯電話機へメールによって送信する動作は、図 16 に示すフローチャートに従って行なっても良い。図 16 に示すフローチャートは、図 15 に示すフローチャートのステップ S304 をステップ S303 に代え、かつ、その代えたステップ S303 とステップ S306 との間にステップ S305 を挿入したものであり、その他は図 15 に示すフローチャートと同じである。携帯電話機 100 のコントローラ 1106 は、メモリカード 110 からコンテンツ情報 420 を読出し、そのコンテンツ情報をメール作成部 1226 へ与えると、メール作成部 1226 は、タグとともにコンテンツ情報 420 をメール本体に付加してコンテンツメールを作成する（ステップ S303）。

【0173】そして、コントローラ 1106 は、既にメモリカード 110 から読出したファイルヘッダ 410 に含まれるコンテンツ ID を抽出し、コンテンツ ID をメール作成部 1226 に与える。メール作成部 1226 は、受取ったコンテンツ ID を字間、字体等を調整してメール本体に付加する（ステップ S305）。

【0174】ここで、「タグ」とは、ユーザがコンテンツメールを見て、そのコンテンツメールの情報を対象として操作を行なえるようにするための制御信号である。タグの利用方法としては、コンテンツメールを受信した携帯電話機 120 のユーザが携帯電話機 100 のユーザと同じコンテンツファイル（暗号化コンテンツデータ）

のダウンロードを希望する場合、コンテンツメールからタグを参照し、コンテンツIDを抽出することによって、暗号化コンテンツデータのダウンロード時にコンテンツIDを取得する過程を省略することが考えられる。その後、図15に示すステップS306、S308、S310、S312と同じ動作が行なわれてコンテンツメールの携帯電話機100から携帯電話機120への送信は終了する。

【0175】コンテンツ情報に加え、タグとともにコンテンツIDを付加して作成したコンテンツメールを送信する場合、表示機能や操作機能の貧弱な携帯電話機におけるユーザの負荷を軽減できるとともに、ユーザがコンテンツファイル（暗号化コンテンツデータ）、およびそのライセンスを配信サーバからダウンロードする際に必要となるコンテンツIDの取得処理を軽減することができる。

【0176】また、上記においては、携帯電話機100のユーザがキー操作部1108からコンテンツ情報のメールによる送信を要求する場合について説明したが、本発明は、かかる場合に限られず、携帯電話機120のユーザが携帯電話機100へコンテンツ情報の送信を要求し、携帯電話機100がコンテンツ情報を携帯電話機120へ送信する場合であっても良い。この場合、携帯電話機100のコントローラ1106は、送受信部1104からコンテンツ情報の送信要求を受取ると、図15または図16に示すフローチャートに従ってコンテンツメールを作成し、その作成したコンテンツメールを携帯電話機120へ送信する。こうにすることによって、携帯電話機のユーザ間においてコンテンツ情報を自由にやり取りすることができ、ユーザの負荷を一層軽減できる。

【0177】なお、上記においては、暗号化コンテンツデータを対象として説明したが、本発明は暗号化コンテンツデータに限らず、暗号化されていないコンテンツデータも対象とする。また、携帯電話機を例にして暗号化コンテンツデータの配信、再生、およびコンテンツ情報のメールについて説明したが、本発明は携帯電話機に限らず、他の携帯端末装置であっても良い。

【0178】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信

のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 ライセンスサーバの構成を示す概略ブロック図である。

【図6】 図5に示すライセンスサーバの情報データベースの構成図である。

【図7】 コンテンツファイルの構成図である。

【図8】 携帯電話機の構成を示すブロック図である。

【図9】 メモリカードの構成を示すブロック図である。

【図10】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図11】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図12】 携帯電話機における再生動作を説明するための第1のフローチャートである。

【図13】 携帯電話機における再生動作を説明するための第2のフローチャートである。

【図14】 コンテンツメールを送信するシステムを概念的に説明する概略ブロック図である。

【図15】 図14に示すシステムにおいてコンテンツメールの送信動作を説明するフローチャートである。

【図16】 図14に示すシステムにおいてコンテンツメールの送信動作を説明する他のフローチャートである。

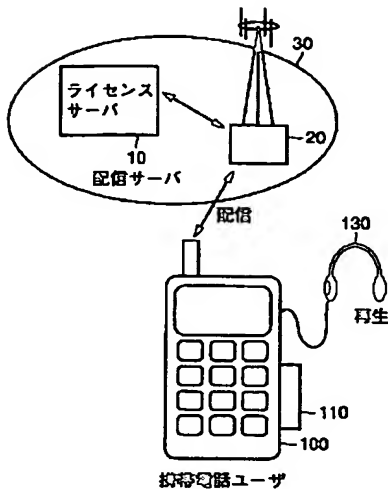
【符号の説明】

10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、40 記録媒体、41 コンテンツファイル、410 ファイルヘッダ、411 UDAC Code、412 プロトコルバージョン、413 コンテンツID、414 コンテンツバージョン、415 ファイル長、416 ContentType、417 Play Time、418 Number of Data Objects、419 Information Length、420 コンテンツ情報、421 曲名、422 アーティスト名、430 データテーブル、440~44n コンテンツデータ、100、120 携帯電話機、110、140 メモリカード、130 ヘッドホン、1106、1420 コントローラ、302 課金データベース、304 情報データベース、306 CRLデータベース、310 データ処理部、312、320、1206、1212、1214、1404、1406、1408、1412、1422 復号処理部、315 配信制御部、316、1210、1418 セッションキー発生部、318、326、328、1208、1410 暗号処理部、350 通信装置、1102 アンテナ、1104 送受信部、1108 キー操作部、1110 ディスプレイ、1112 音声再生部、1113、1218 DA変換器、11

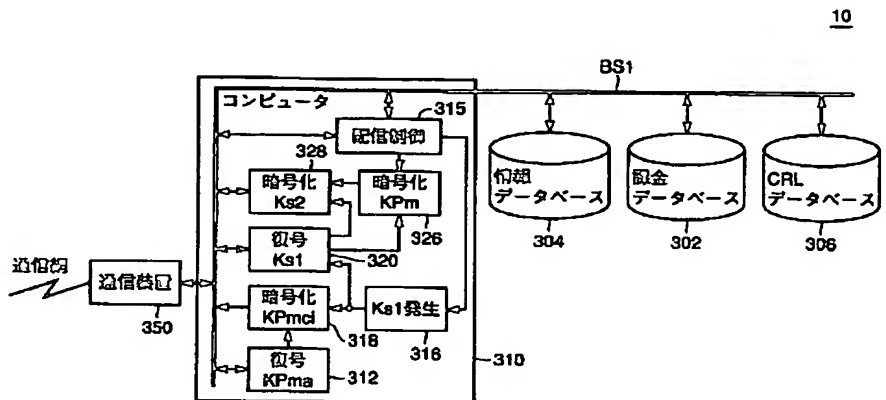
14, 1201, 1220, 1224 端子、1200
メモリインタフェース、1202, 1400 認証デ
ータ保持部、1204 Kp1保持部、1216 音楽
再生部、1222 スイッチ、1226 メール作成

部、1402Kmc1保持部、1414 KPma保持
部、1415 メモリ、1416KPm1保持部、14
21 Km1保持部、1440 ライセンス情報保持
部、1442, 1444, 1446 切換スイッチ。

【図1】



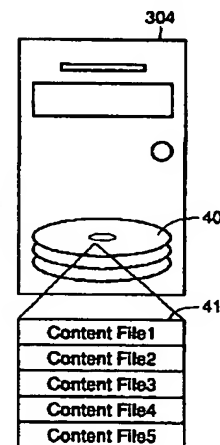
【図5】



【図2】

名称	属性	保持/発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例: 音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバより配布。
Data-Inf	付加情報		例: コンテンツデータに関する著作権あるいは サーバアクセス回数等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可)
AC	ライセンス購入条件		利用者側から相定(例: ライセンス取得回数等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例: 再生可能回数)
AC2	再生回数制御情報		コンテンツ再生回数(携帯電話機)における制限情報 (例: 再生可否)

【図6】



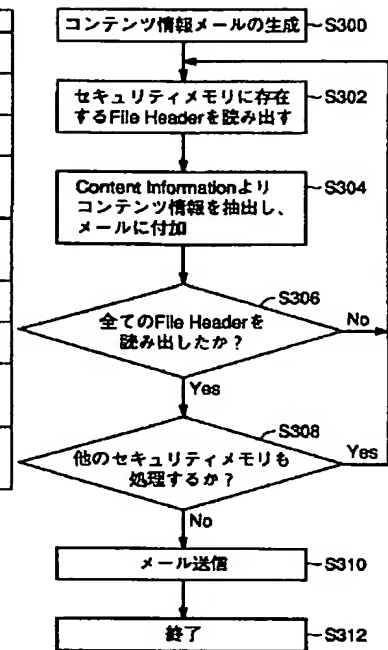
【図4】

名称	属性	保持/発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信/再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵 (非対称鍵)	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。

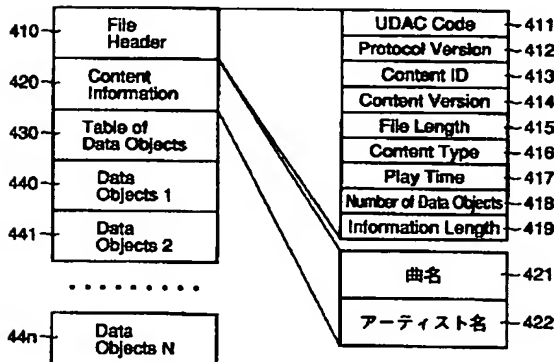
【図 3】

名称	属性	保持/発生箇所	機能・特徴
CRL	禁止クラスリスト 関連情報	配信サーバ メモ리카ード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報 (差分データ形式)
CRL_ver		メモ리카ード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 (非対称鍵)	携帯電話機	Kpniにて復号可能。 (KPpn/Crtin)KPmaの形式で出荷時に記録 *携帯電話機の種類nごとに異なる。
KPmcl	公開暗号鍵 (非対称鍵)	メモ리카ード	Kmclにて復号可能。 (KPmcl/Cmcl)KPmaの形式で出荷時に記録 *メモ리카ードの種類iごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 *携帯電話機の種類nごとに異なる。
Kmcl	秘密復号鍵	メモ리카ード	メモ리카ード固有の復号鍵 *メモ리카ードの種類iごとに異なる。
Crtin	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 (KPpn/Crtin)KPmaの形式で出荷時に記録 *携帯電話機のクラスnごとに異なる。
Cmcl		メモ리카ード	メモ리카ードのクラス証明書。認証機能を有する。 (KPmcl/Cmcl)KPmaの形式で出荷時に記録 *メモ리카ードのクラスiごとに異なる。

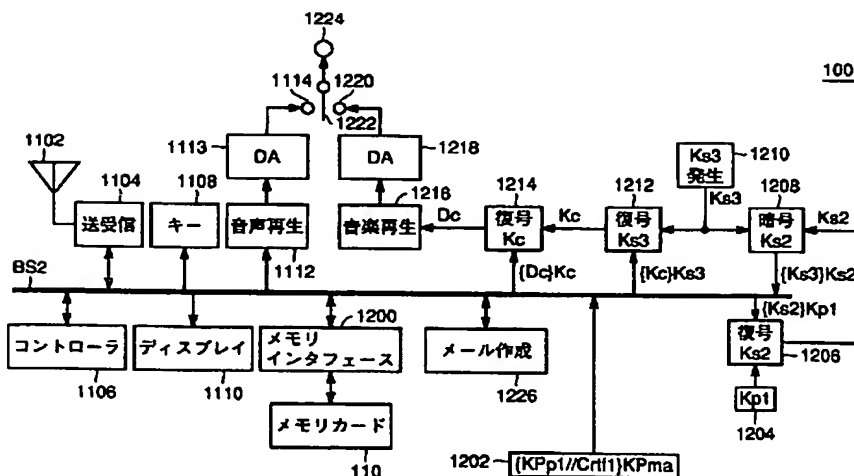
【図 15】



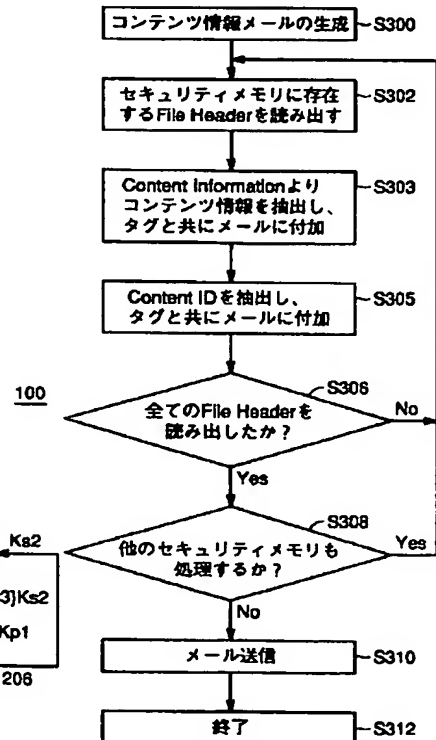
【図 7】



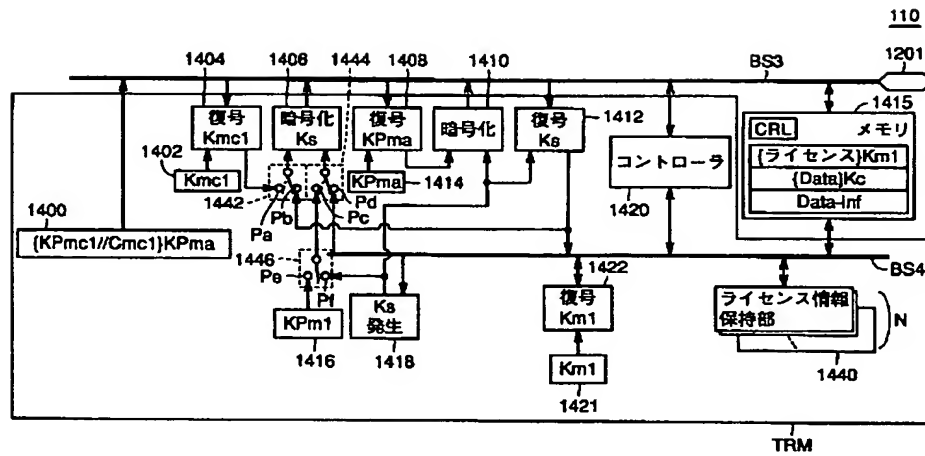
【図 8】



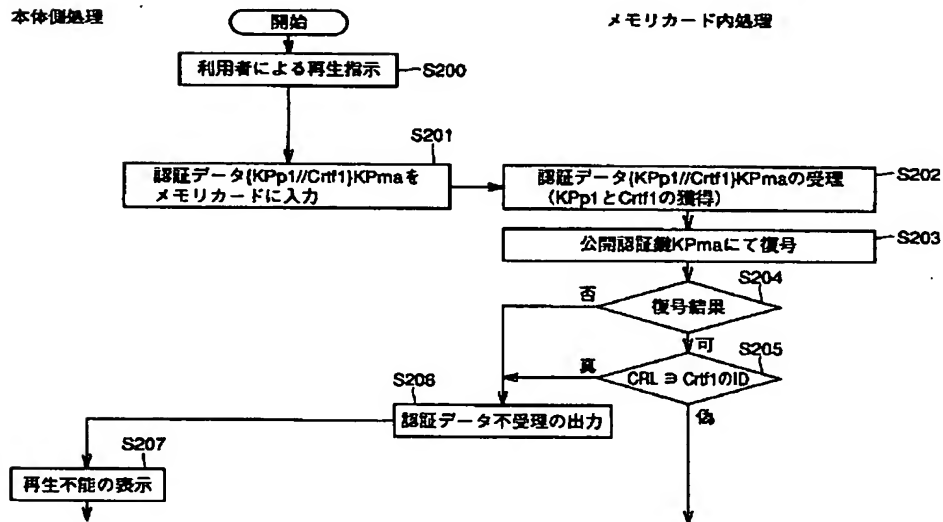
【図 16】



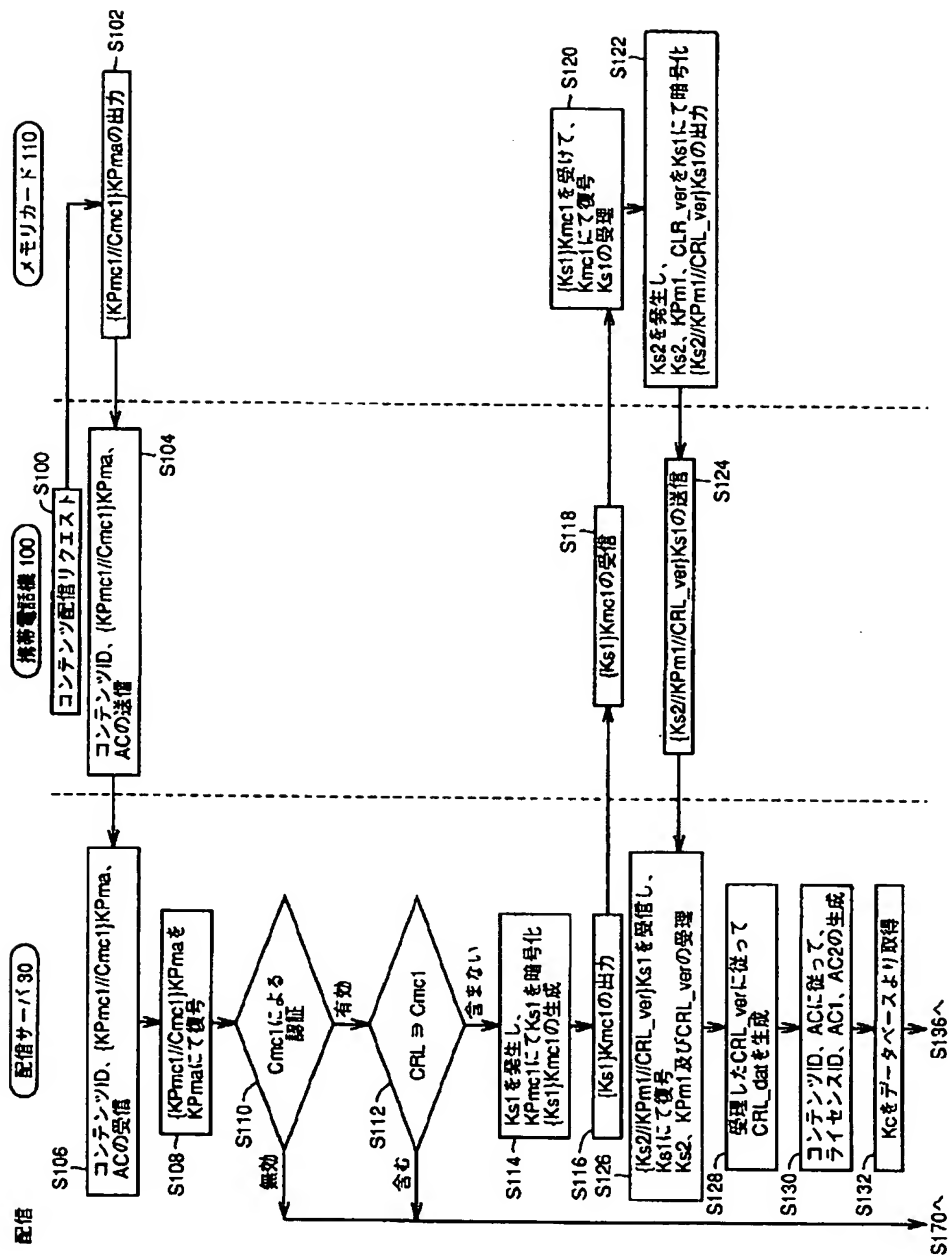
【図 9】



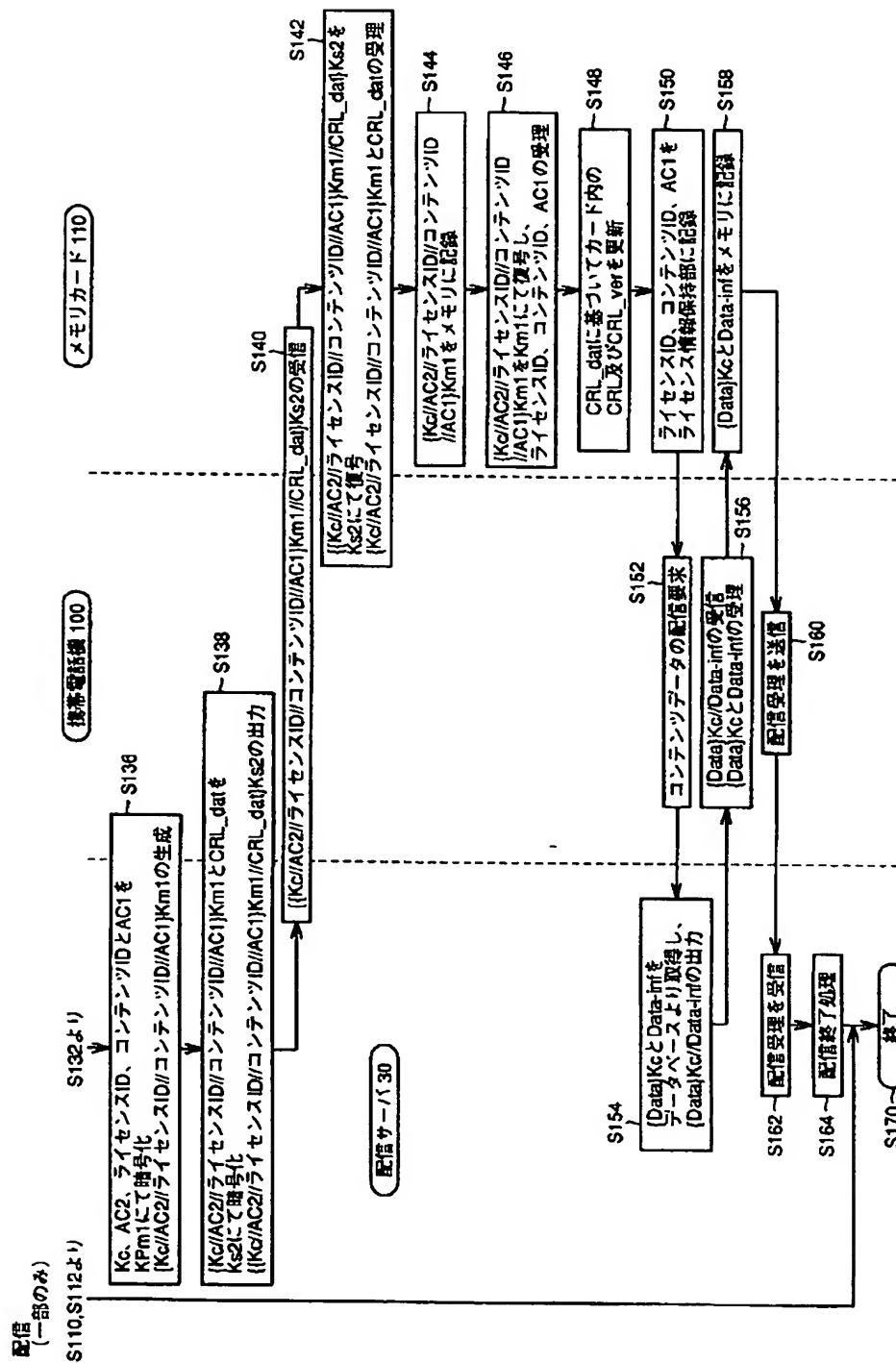
【図 12】



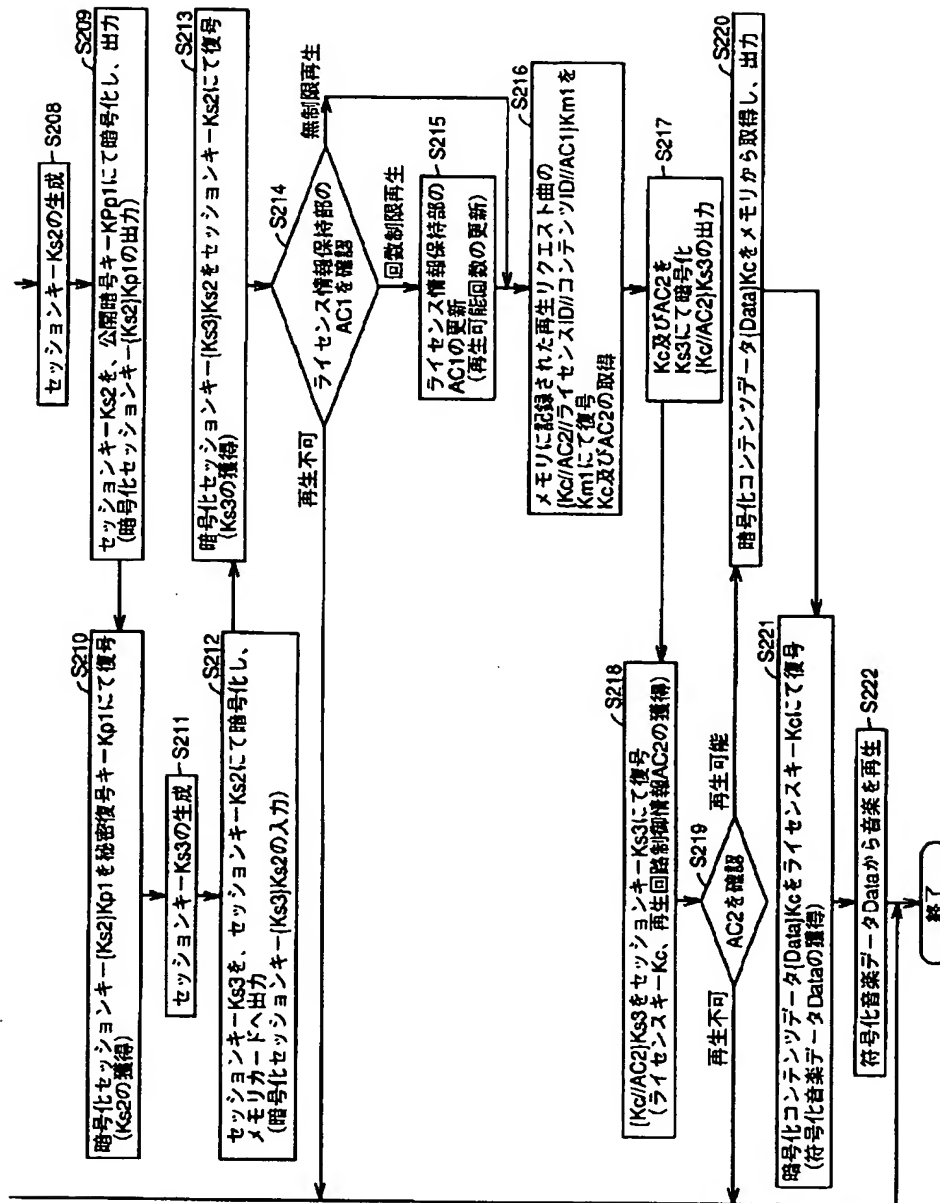
【図10】



【図 11】



【図13】



【図 14】

